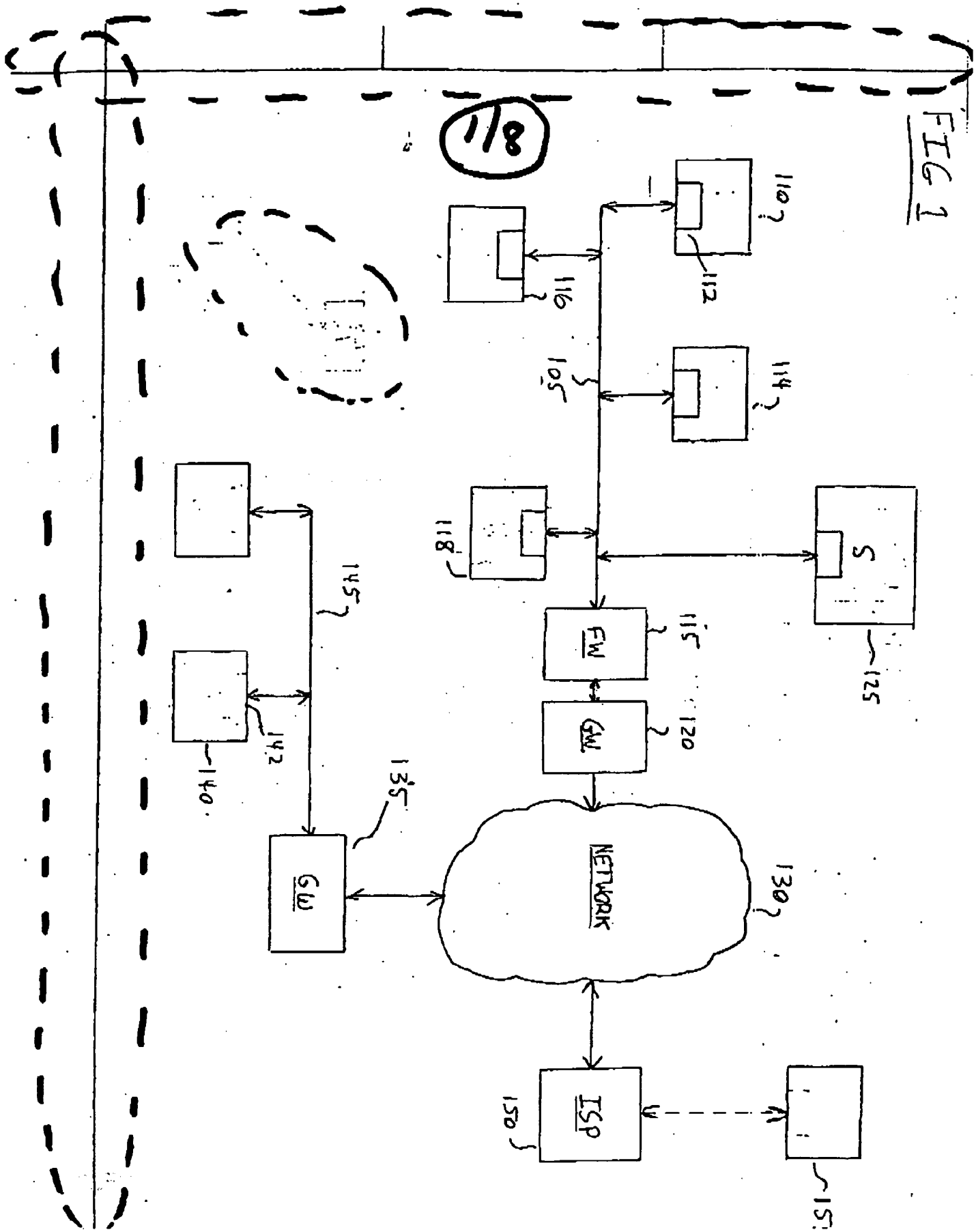
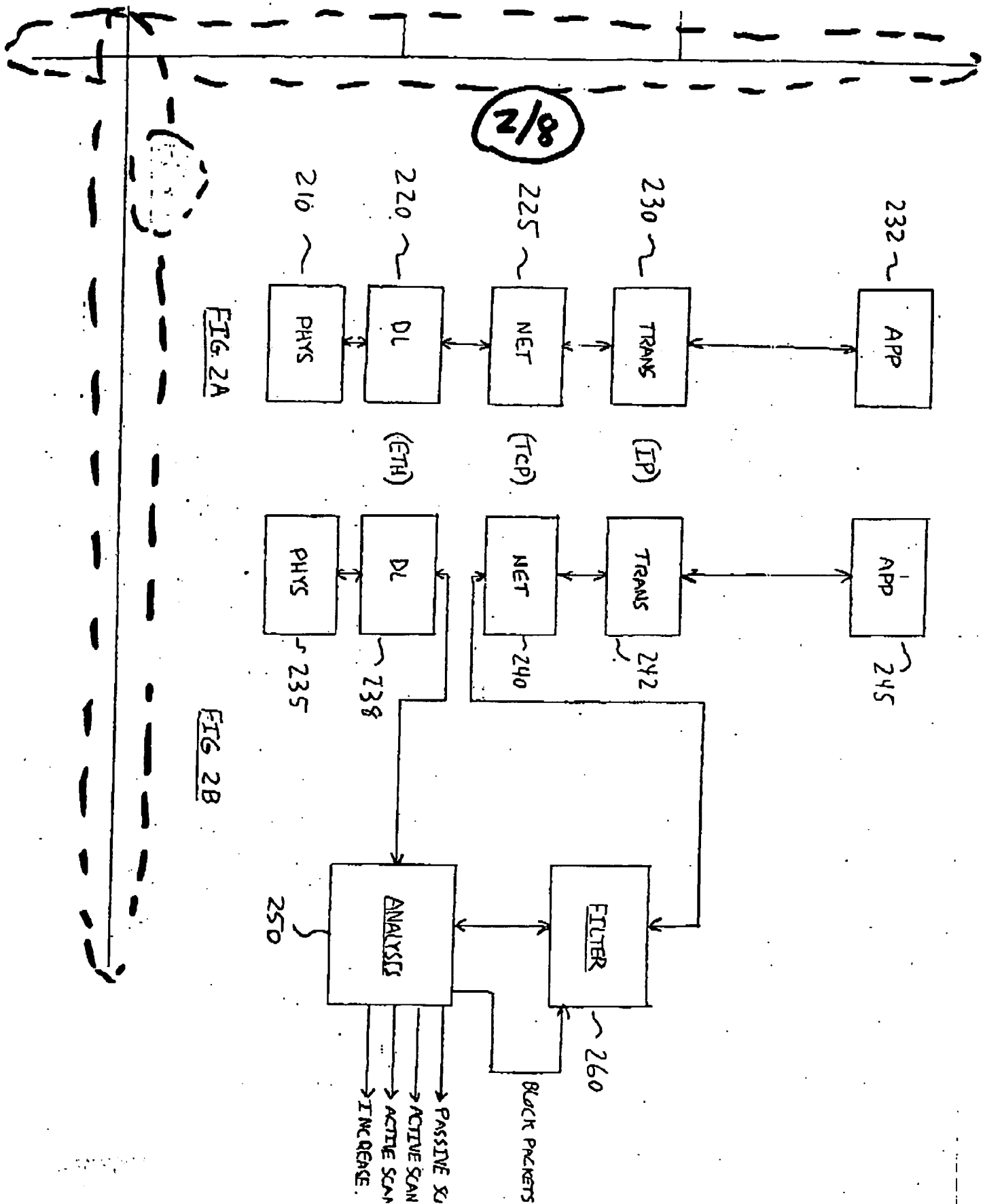
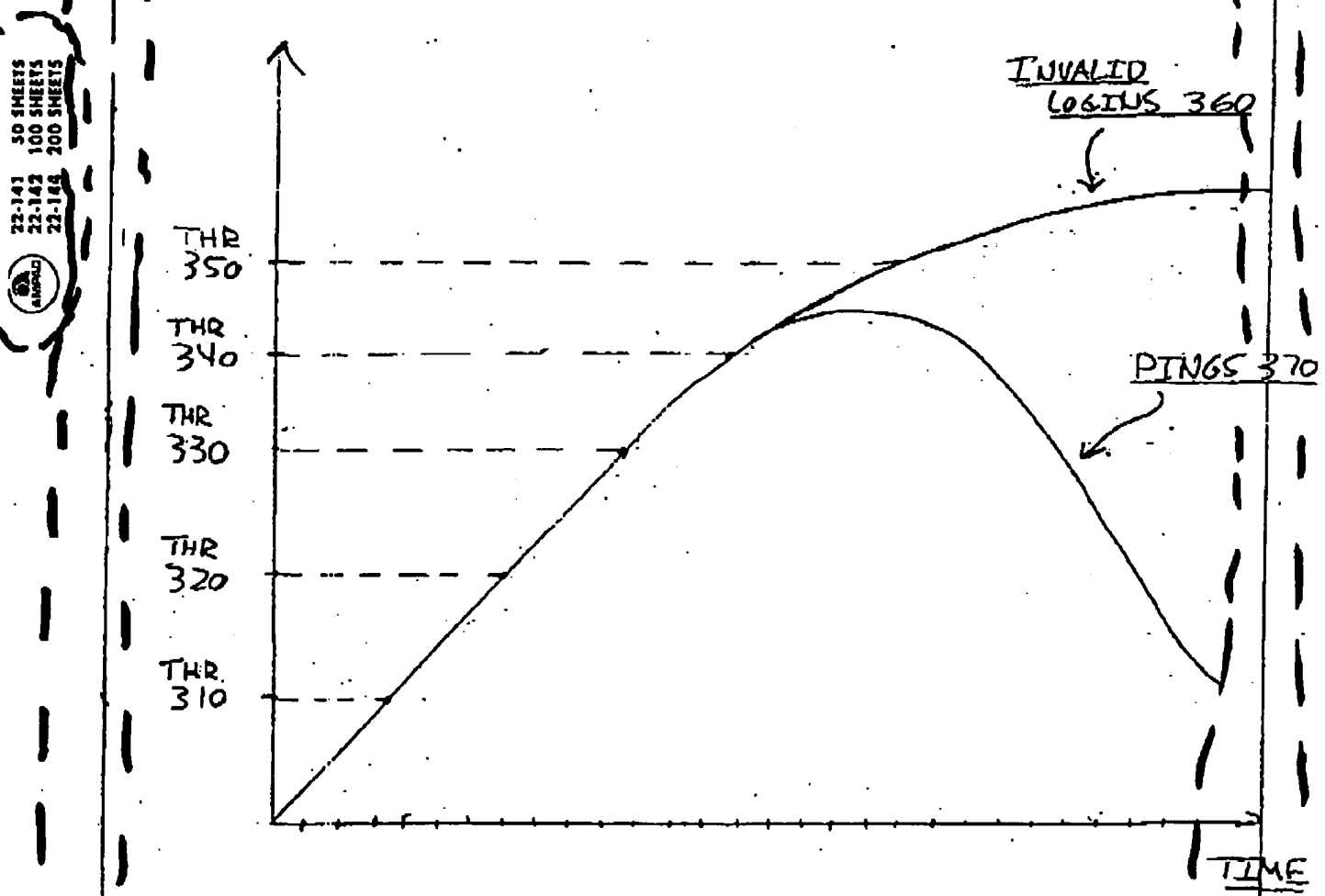

1/8
FIG 1
110
112
116
114
105
118
S
121
115
FM
120
GW
125
135
GW
NETWORK
130
ISP
150
151
140
142
145

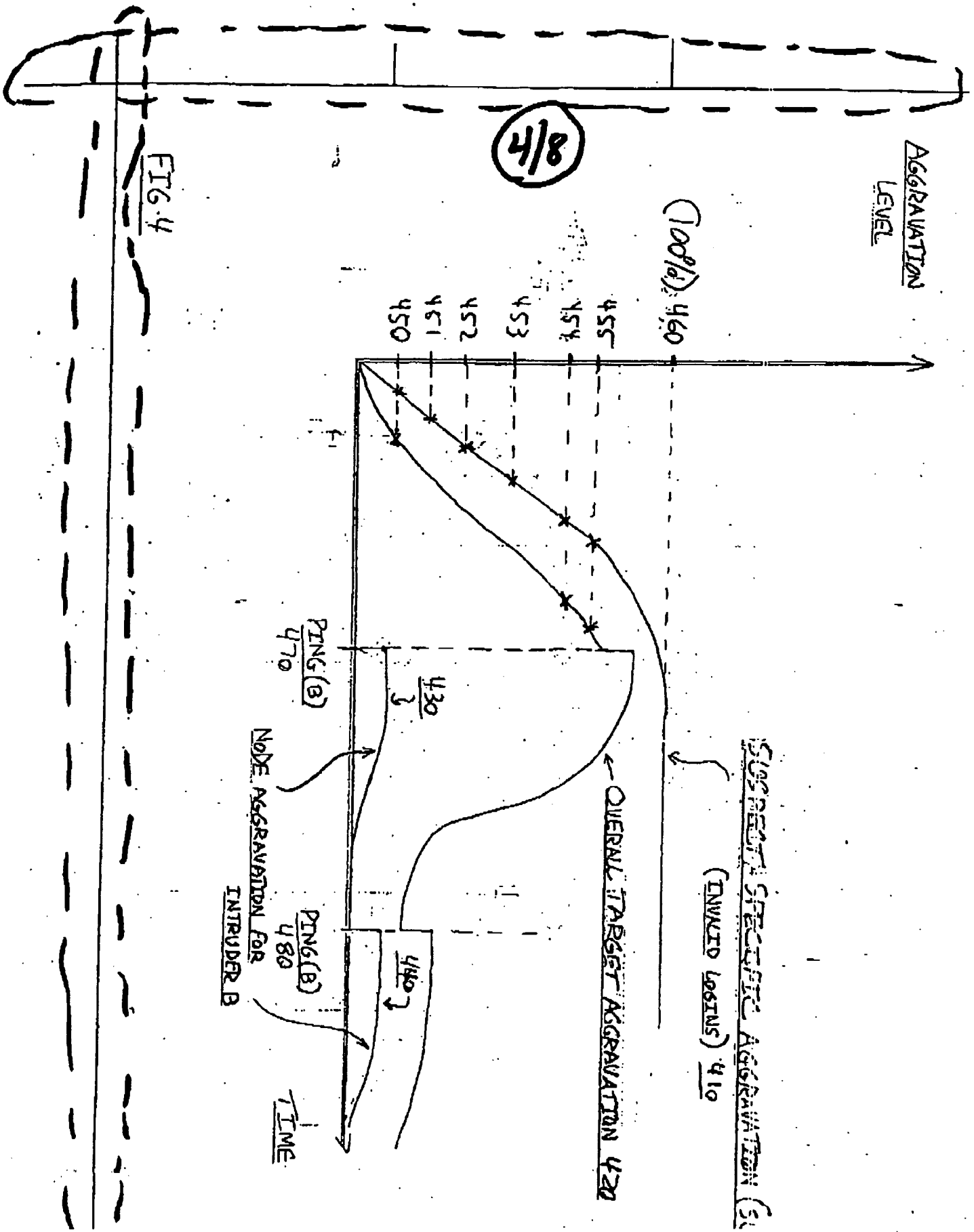

2/8
210
220
225
230
232
PHYS
DL
NET
TRANS
APP
(ETH)
(TCP)
(IP)
FIG. 2A
235
238
240
242
245
PHYS
DL
NET
TRANS
APP
FIG 2B
250
ANALYSIS
FILTER
260
INCREASE
ACTIVE SCAN
PASSIVE SCAN
BLOCK PACKETS

3/8

FIG 3

p 13


INVALID LOGINS 360
PINGS 370
THR 350
THR 340
THR 330
THR 320
THR 310
TIME
INCIDENTS


4/8
FIG. 4
AGGRAVATION LEVEL
(log)
05h
15h
25h
35h
45h
55h
60h
PING (B) 470
NODE AGGRAVATION FOR INTRUDER B
PING (B) 480
TIME
QUERALL TARGET AGGRAVATION 420
(INVALID LOGINS) 410

5/8

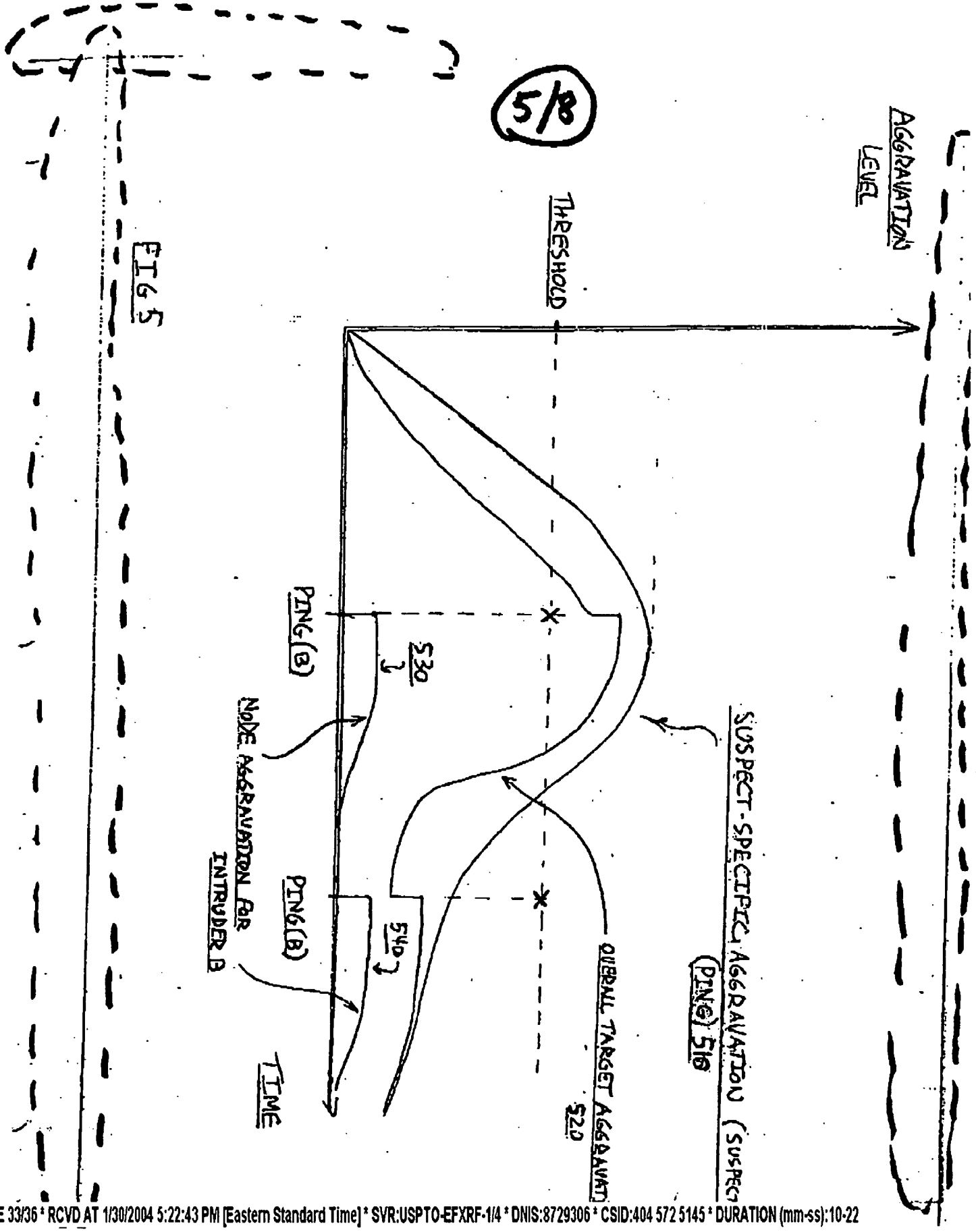

AGGRAVATION LEVEL
THRESHOLD
PING(a)
PING(b)
TIME
NODE AGGRAVATION FOR INTRUDER B
SUSPECT-SPECIFIC AGGRAVATION (SUSPECT)
OVERALL TARGET AGGRAVATION
520
530
540
510

FIG 5

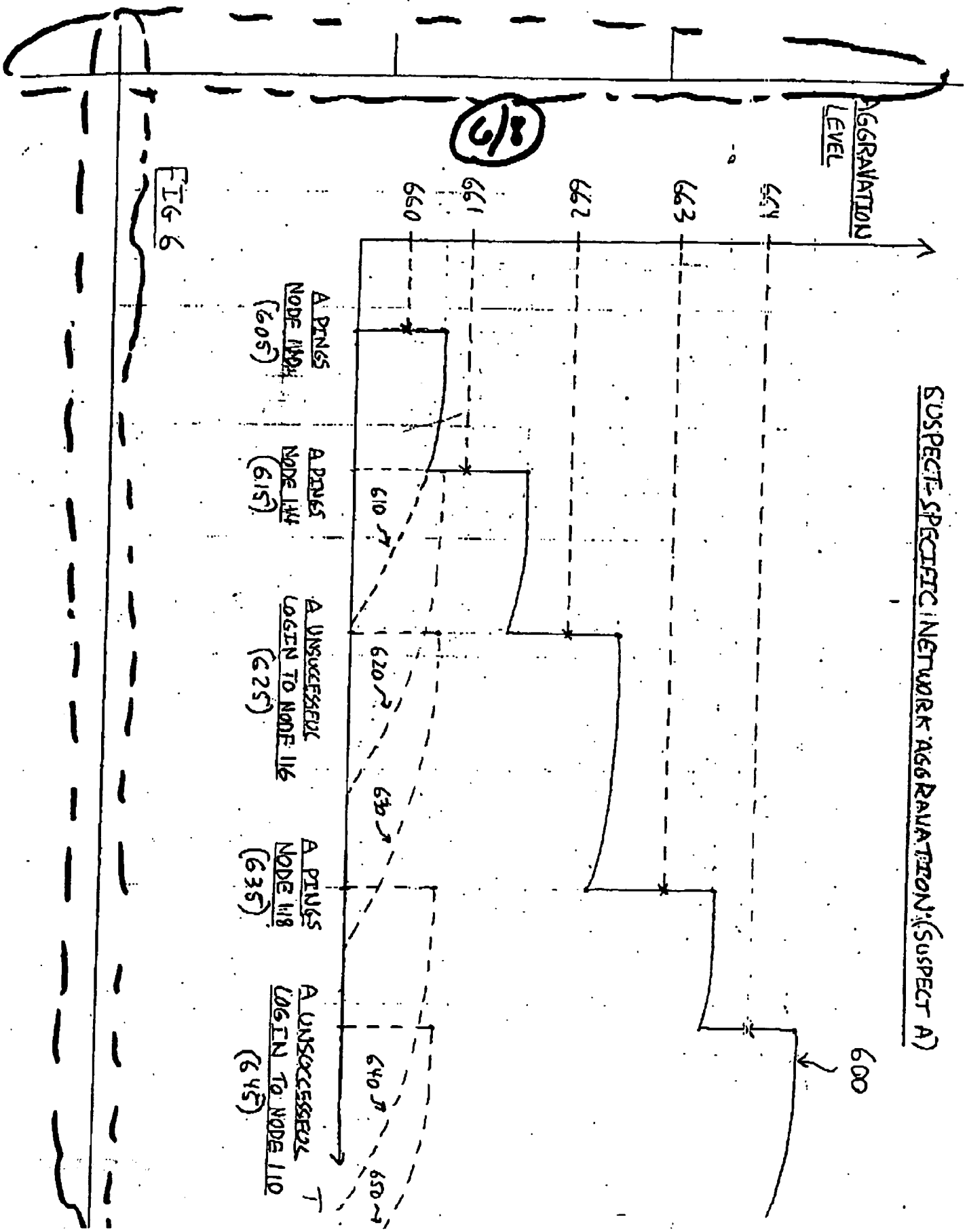

6/8
FIG 6
AGGRAVATION LEVEL
660
661
662
663
664
A PINGS NODE 114 (605)
A PINGS NODE 114 (615)
A UNSUCCESSFUL LOGIN TO NODE 116 (625)
A PINGS NODE 118 (635)
A UNSUCCESSFUL LOGIN TO NODE 110 (645)
610
620
630
640
650
600
SUSPECT-SPECIFIC NETWORK AGGRAVATION (SUSPECT A)

FIG 7

7/8

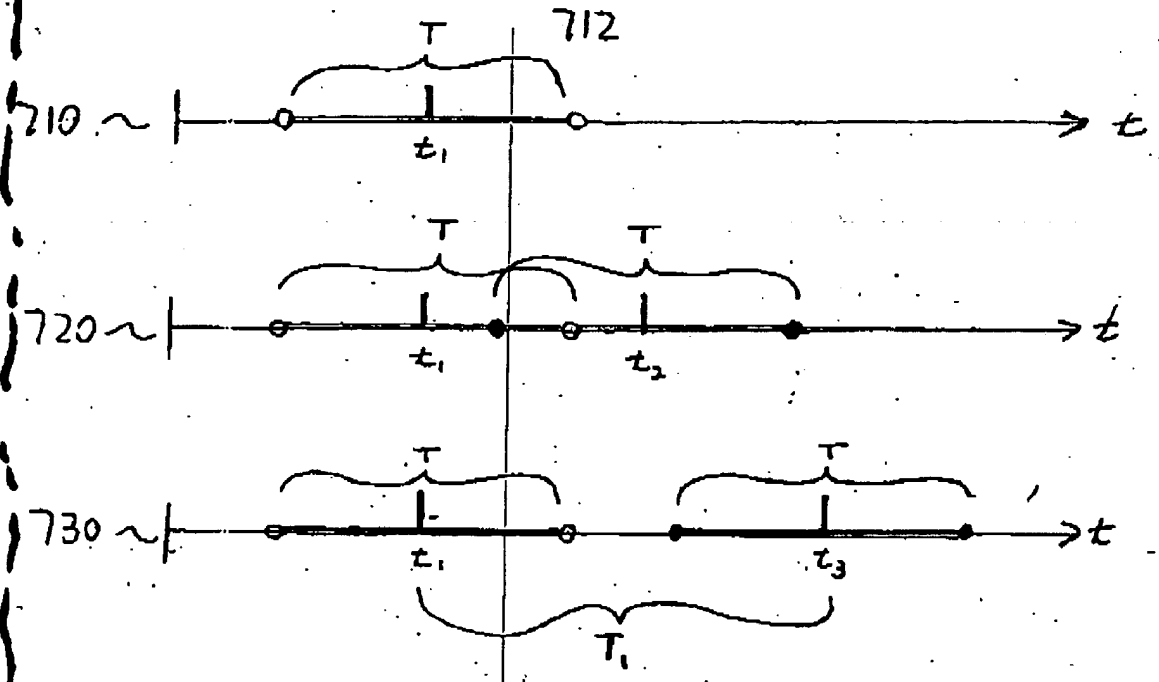
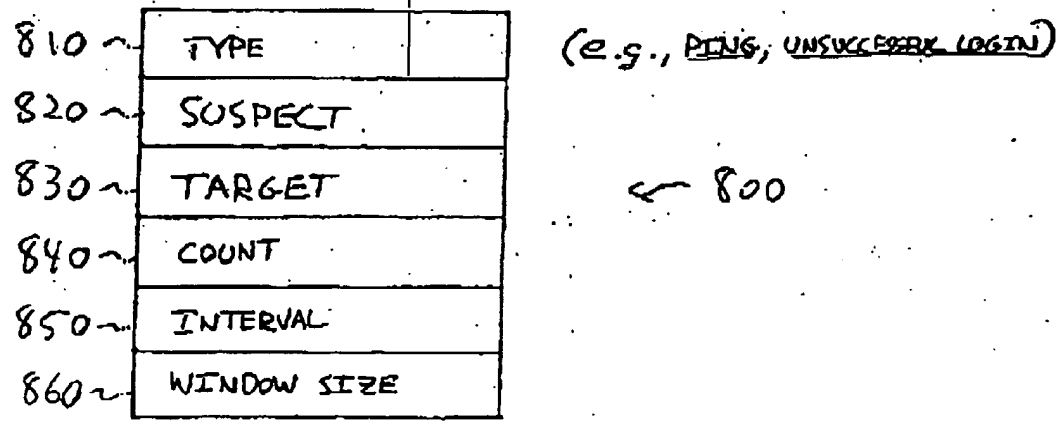

T
712
710
t
t_1
T
T
720
t
t_1
t_2
T
T
730
t
t_1
t_3
T_1

FIG 8


810
TYPE
(e.g., PING, UNSUCCESSFUL LOGIN)
820
SUSPECT
830
TARGET
800
840
COUNT
850
INTERVAL
860
WINDOW SIZE

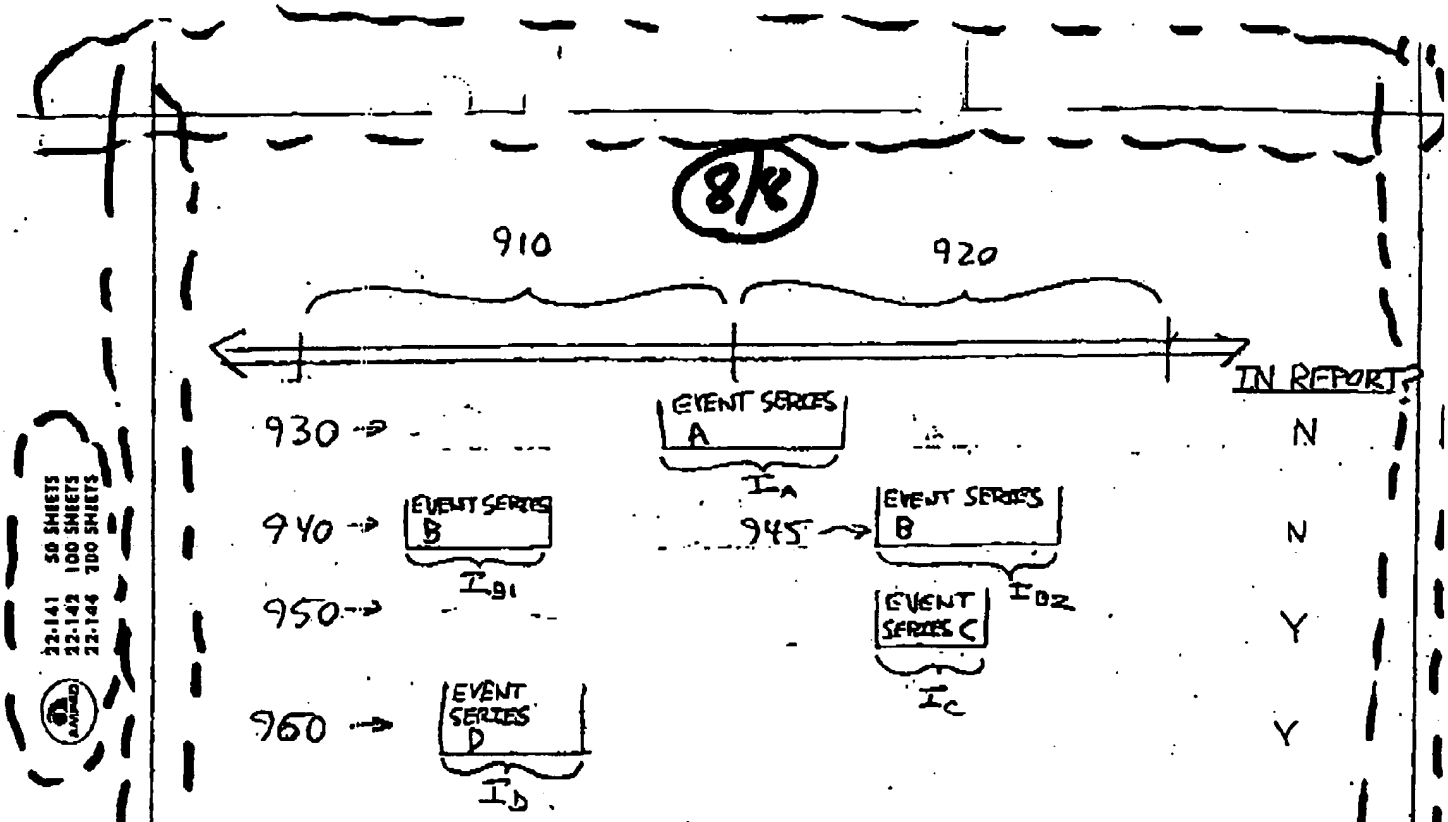

8k
910
920
IN REPORT?
930
EVENT SERIES A
I_A
940
EVENT SERIES B
I_{B1}
945
EVENT SERIES B
I_{B2}
950
EVENT SERIES C
I_C
960
EVENT SERIES D
I_D
N
N
Y
Y

FIG 9.